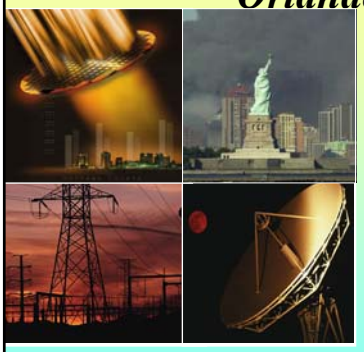
An Energy-Efficiency Workshop and ~~Exposition~~
Orlando, Florida



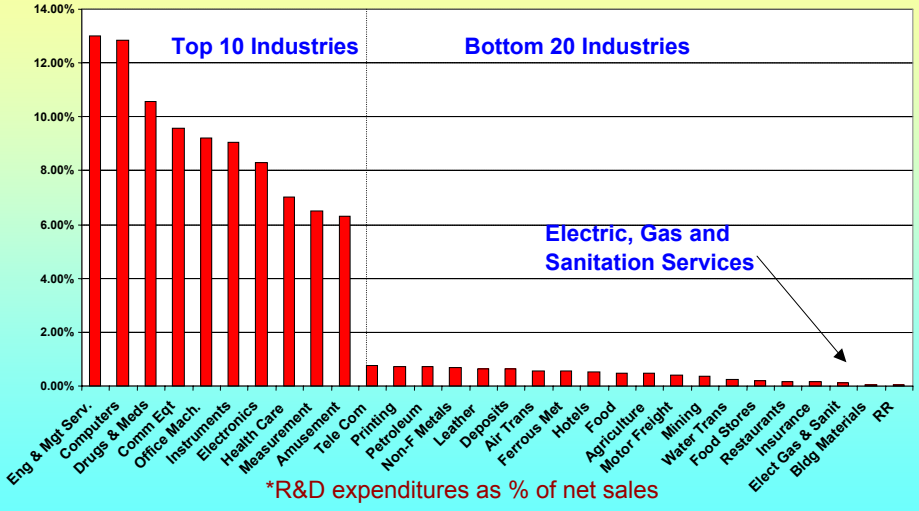
Security & Resilience of Energy Infrastructure

Massoud Amin, D.Sc.
H.W. Sweatt Chair in Technological Leadership
Director, Center for Dev. of Tech. Leadership
Professor, Electrical & Computer Engineering
University of Minnesota, Twin Cities

Most of the material and findings for this presentation were developed while the author was at the Electric Power Research Institute (EPRI) in Palo Alto, CA. EPRI's support and feedback from colleagues at EPRI is gratefully acknowledged.

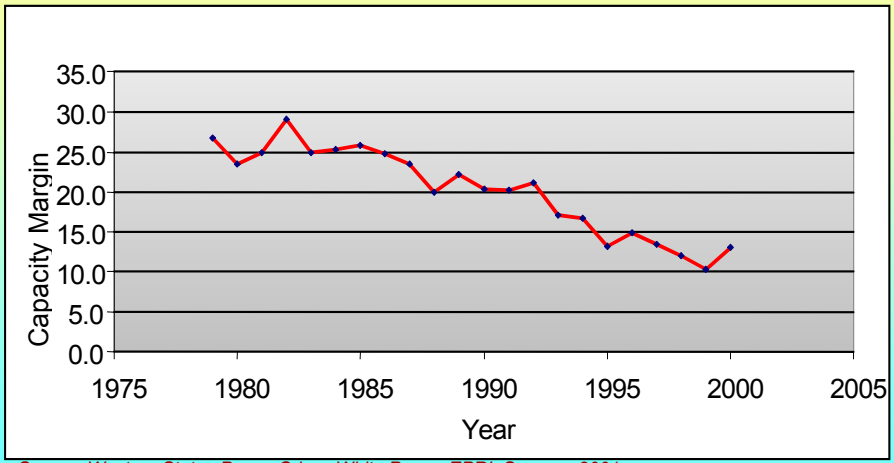
The vast networks of electrification are the greatest engineering achievement of the 20th century.
-- *U.S. National Academy of Engineering*

Context: R&D Expenditures*



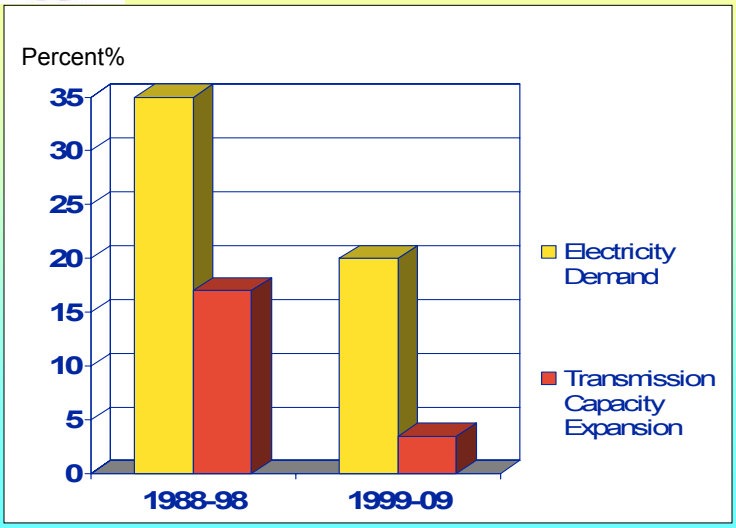
*R&D expenditures as % of net sales

Context: Generation Capacity Margin in North America

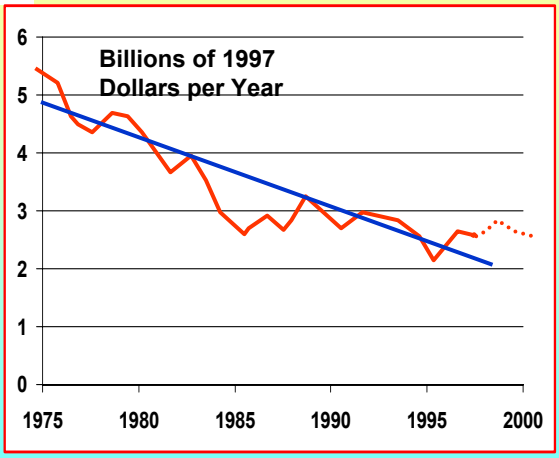


Source: Western States Power Crises White Paper, EPRI, Summer 2001

Context: Transmission Additions in The U.S.

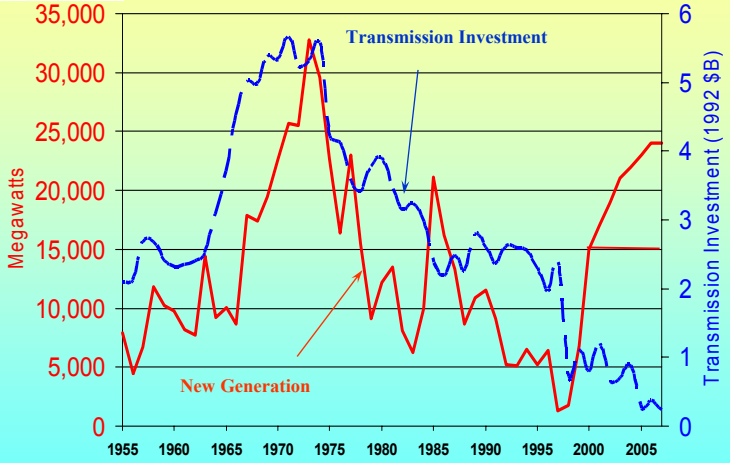


Context: Transmission Investment, 1975-2000



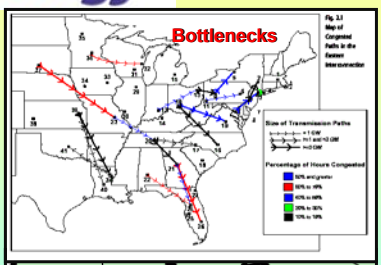
Source: Electric Perspectives, July/August 2001

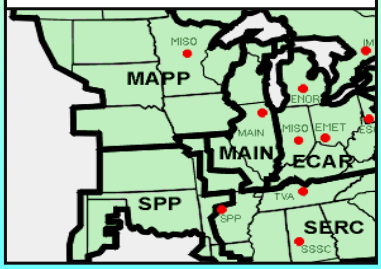
Past Practice is Inadequate

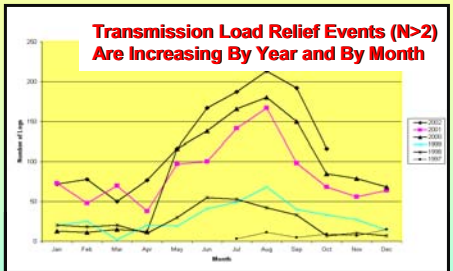


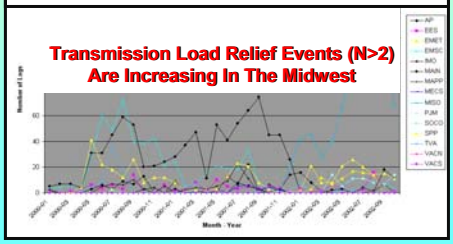
- **Many more bottlenecks showing up**

Transmission Bottlenecks Are Impacting Interconnected Regions



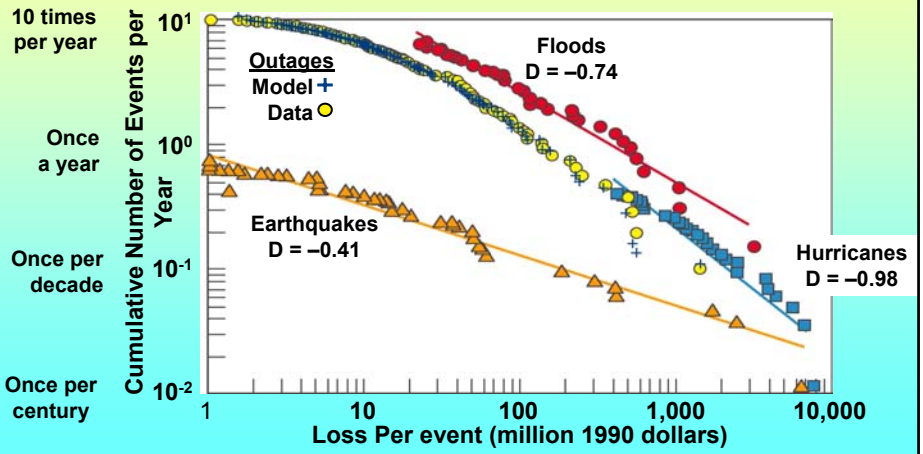






Power Law Distributions: Frequency & impacts of major disasters

Hurricane and Earthquake Losses 1900–1989
Flood Losses 1986–1992
Electric Network Outages 1984–2000

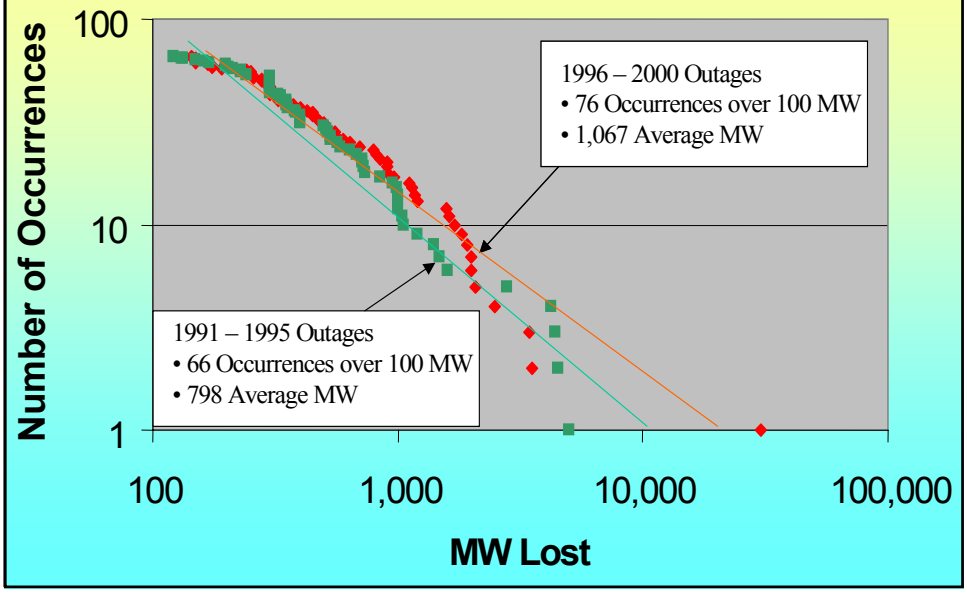


Vulnerabilities of Power Grid: Examples

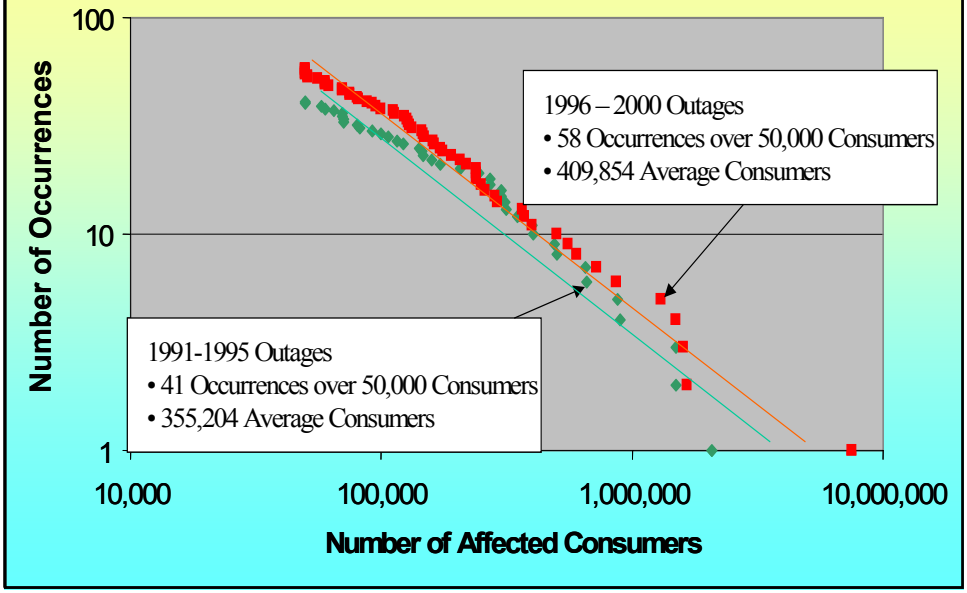
Attention has gradually increased after several cascading failures:

- November 1965 blackout in the Northeast U.S., which cascaded system collapse in ten states.
- 1967 Pennsylvania-New Jersey-Maryland.
- July 13, 1977 blackout in New York City.
- December 19, 1978 blackout due to voltage collapse in France.
- July and August 1996 outages in the western U.S. grid.
- Summers' 98-'01 price spikes (infrastructure's inadequacy affecting markets).
- December 1998, Bay Area black-out. New York's July 7, 1999 blackout.
- Industry-wide Y2K readiness program identified telecommunications failure as the biggest source of risk of the lights going out on rollover to 2000.
- Western States' power crises in summer 2001 and its aftermath…
- Eastern United States and Canada cascading outages on August 14th, 2003.

Historical Analysis of U.S. outages in terms of the amount of electric load lost (1991-2000)



Historical Analysis of U.S. outages in terms of Affected Customers (1991-2000)



Cascading Failures of August 14th, 2003: NERC is establishing teams to study the event and will coordinate with FERC, DOE, the industry and others. Source: "Preliminary Disturbance Report of the 8/14/03 Sequence of Events", NERC (8/1503, 6:20 pm EDT)

Preliminary NERC report:

3:06 pm EDT: Chamberlain – Harding 345kV line tripped
Cause not reported

3:32 pm EDT: Hanna – Juniper 345kV line sagged & tripped

3:41 pm EDT: Star – S. Canton 345 kV line tripped (Ohio)

3:46 pm EDT: Tidd – Canton Ctrl 345 kV line tripped (Ohio)

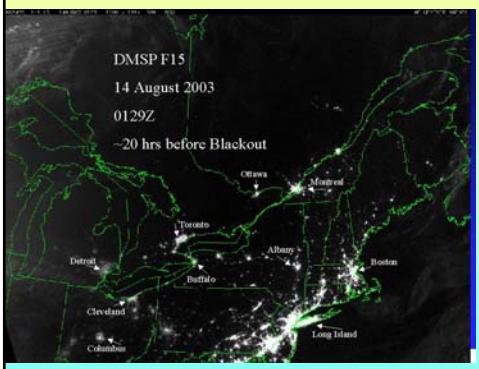
4:06 pm EDT: Sammis – Star 345 kV line tripped and reclosed (Ohio)

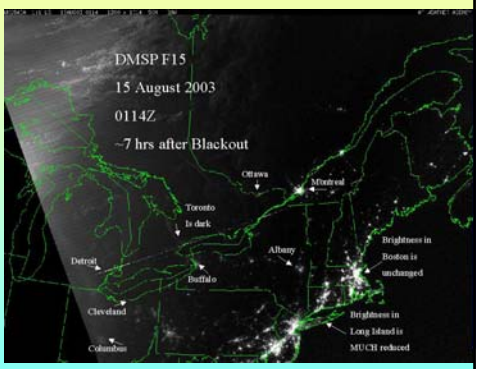
4:10 pm EDT (Michigan): Campbell #3 Tripped?; Hampton – Thetford 345 kV line tripped; Oneida – Majestic 345 kV line tripped

4:11 pm EDT: Avon Unit 9 Tripped; Beaver – Davis Besse; Midway – Lemoyne – Foster 138 (?) kV line tripped; Perry Unit 1 tripped

4:15 pm EDT: Sammis – Star 345 kV line tripped and reclosed
4:17 pm EDT: Fermi Nuclear tripped
4:17 – 4:21 EDT: Numerous lines in Michigan tripped

Cascading failures of August 14th, 2003: ~ 20 hrs before, and 7 hrs after





Source: NOAA
http://www.noaanews.noaa.gov/nightlights/blackout081403-20hrsbefore-text.jpg
http://www.noaanews.noaa.gov/nightlights/blackout081503-7hrsafter-text.jpg

Context: Today's Power System Increasingly Stressed Infrastructure

- Infrastructure expansion has not kept up with demand: generation & transmission capacity margins are shrinking
- Transition to competition is creating new demands
  - Power transactions are growing exponentially
  - Grid capacity is severely limited
  - Power disturbances cost customers $120 billion/yr
- Technology can meet these demands, but uncertainties on ROI are discouraging investments
- Many distribution systems have not been updated with current technology
- Proliferation of distributed resources – little DR is connected to the grid

- **National infrastructure security assessment adds to concern**

Context: Threats to Physical Security

- Transformers, line reactors, series capacitors, transmission lines...
- Protection of ALL the widely diverse and dispersed assets is impractical
  - 202,835 miles of EHV lines (230 kV and above)
  - 6,644 transformers in Eastern Interconnection alone
- Control Centers
- Interdependence to other Infrastructures
  - Gas pipelines, compressor stations, etc.
  - Dams
  - Rail lines
  - Telecom – monitoring & control of system
- Combinations of the above

Major Threats to the Power System

- Physical attacks on facilities or physical attacks on transmission towers, substations or generating stations
  - Truck bombs
  - Small airplanes
  - Gun shots – line insulators, transformers
  - Hijacking of control
  - Biological contamination (real or threat)
  - Over-reaction to isolated incidents or threats
- Internet Attacks – 30,000 hits a day at an ISO
- Storms, Earthquakes, Forest fires & grass land fires
- Loss of major equipment – especially transformers…

Example:

September 2002 fires

Biscuit Fire - Cascade Fire (Oregon)

Iron Mountain fire

Hickok fire - 776 acres

Freeway Fire - no threat to SCE facilities

Curve Fire: San Gabriel Canyon Road. 30-Miles N/O Azusa, 10,000 acres

Curb Fire: 19,500 acres

Leona Fire: Midway-Vincent area

Whitmore fire: Kilarc-Deschultes 60kV lost

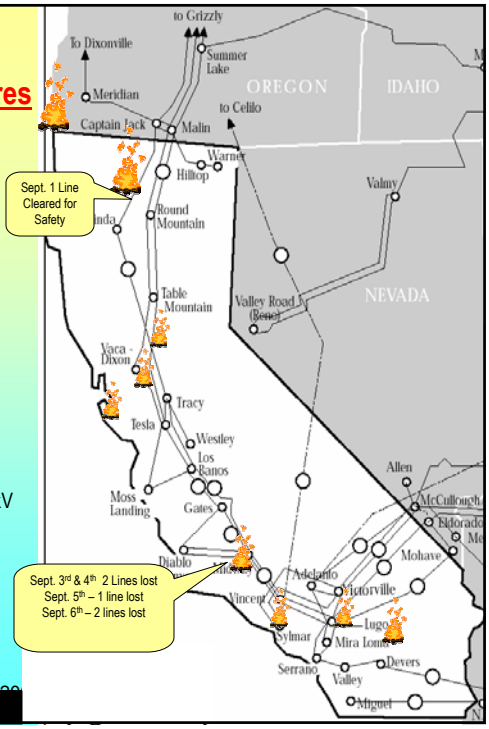
Glendale - Eagle Rock fire: Near Gould-Sylmar 220kV line

Olita Fire: El Dorado County –Gold Hill SS

Mountain Fire: Rutledge - Hardie area

Croy Fire: Morgan Hill area -Metcalf-Green Valley 115kV line impacted

Williams Fire: 35,000 acres



Source CA-ISO

Example: Fire under the 500 kV Lines – Sept 2002

Source CA-ISO

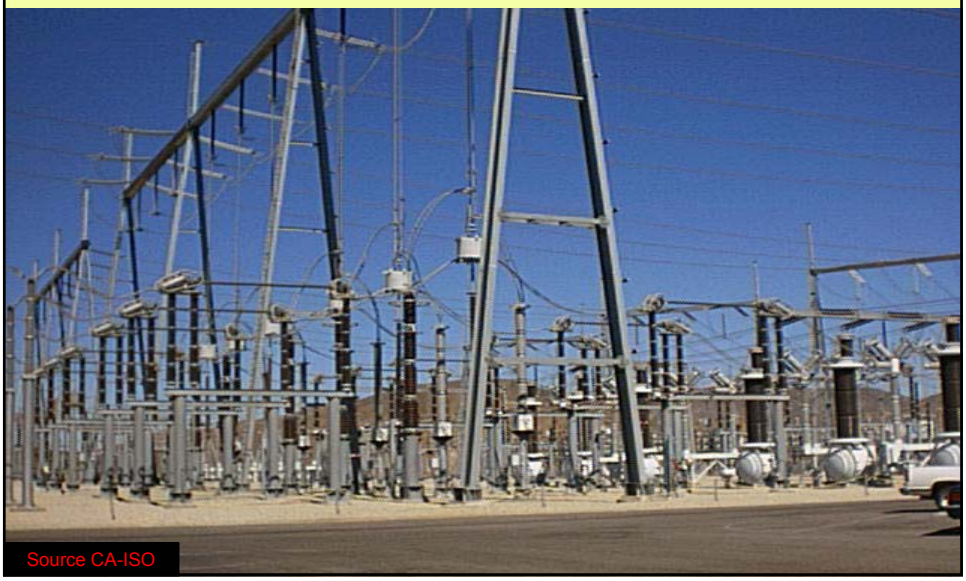
Example: Midway – Vincent 500 kV line tower damage

Source CA-ISO

Midway – Vincent 500 kV line damage

Source CA-ISO

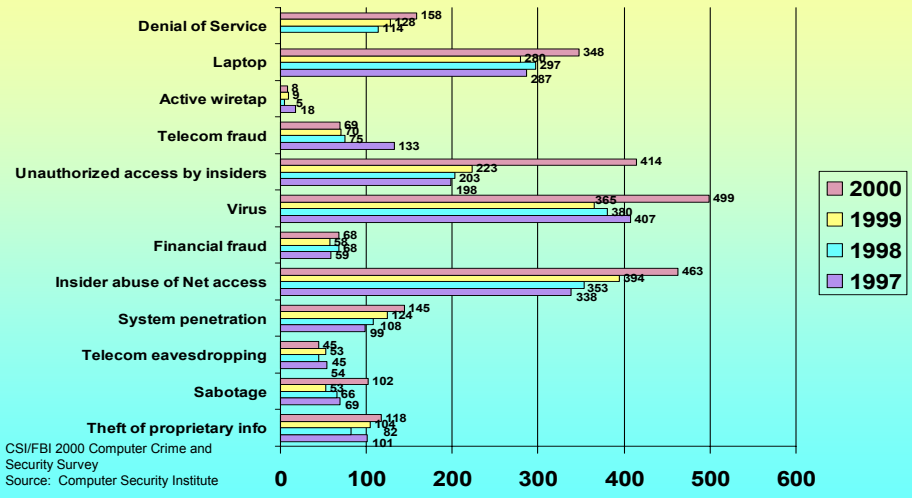
Vincent Substation before Transformer Explosion & Fire



Source CA-ISO

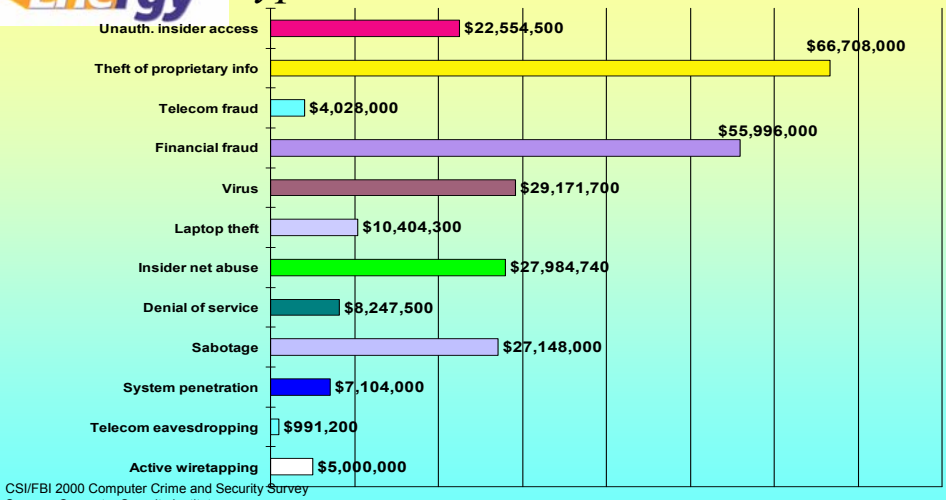
500 / 230 kV Transformer Explosion & Fire: March 21, 2003 Vincent Substation

Context: Types of attack or misuse detected



CSI/FBI 2000 Computer Crime and Security Survey
Source: Computer Security Institute

Context: Dollar amount of losses by type



CSI/FBI 2000 Computer Crime and Security Survey
Source: Computer Security Institute

Context: The Role of Digital Control Systems in the Electric Industry

Today, digital control systems are essential to the reliable operation of the electricity infrastructure

- Supervisory Control & Data Acquisition (SCADA) systems & Energy Management Systems (EMS) control the power flow from generators to end users
- Distributed Control Systems (DCSs) are used to control the operation of generating plants
- Intelligent Electrical Devices (IEDs) & Programmable Logic Controllers (PLCs) are being extensively used in substations and power plants

Context: Operational Systems Issues

- Highly reliable, real-time systems that require secure two-way communication of dynamic data
  - SCADA, EMS, DCS, PLC, etc
- Operational systems designed to maximize performance and flexibility
  - Electronic security was not a significant consideration
  - Electronic security technology can inhibit performance
- Legacy systems assumed not to be vulnerable
  - Web-based and wireless applications can make them vulnerable
- Open systems can be vulnerable

Electric Company Vulnerability Assessment

- Conducted by 4 National Labs and consultant
- Able to assemble detailed map of perimeter
- Demonstrated internal and end-to-end vulnerabilities
- Intrusion detection systems did not consistently detect intrusions
- X-Windows used in unsecured manner
- Unknown to IT, critical systems connected to internet
- Modem access obtained using simple passwords

Much of the above determined from over 1200 miles away

So what are we doing about it?
Security Related Programs within EPRI

1999-2001	**Y2K**→2000-present	2002-present	2001-present
EPRI/DoD Complex Interactive Networks (CIN/SI)	Enterprise Information Security (EIS)	Infrastructure Security Initiative (ISI)	Consortium for Electric Infrastructure to Support a Digital Society (CEIDS)
Underpinnings of Interdependent Critical National Infrastructures Tools that enable secure, robust and reliable operation of interdependent infrastructures with distributed intel. & self-healing	▪ Information Sharing ▪ Intrusion/Tamper Detection ▪ Comm. Protocol Security ▪ Risk Mgmt. ▪ Enhancement ▪ High Speed Encryption	**Response to 9/11 Tragedies** ▪ Strategic Spare Parts Inventory ▪ Vulnerability Assessments ▪ Red Teaming ▪ Secure Communications	▪ Self Healing Grid

Recent Directions: EPRI/DOD Complex Interactive Network/Systems Initiative

"We are sick and tired of them and they had better change!"
Chicago Mayor Richard Daley on the August 1999 Blackout

Complex interactive networks:

- ***Energy infrastructure*:** Electric power grids, water, oil and gas pipelines
- ***Telecommunication:*** Information, communications and satellite networks; sensor and measurement systems and other continuous information flow systems
- ***Transportation and distribution networks***
- ***Energy markets, banking and finance***

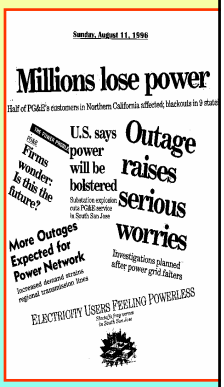
1999-2001: $5.2M / year — Equally Funded by DoD/EPRI

Develop tools that enable secure, robust and reliable operation of interdependent infrastructures with distributed intelligence and self-healing abilities

EPRI/DOD Complex Interactive Network/Systems (CIN/S) Initiative

The Reason for this Initiative: "Those who do not remember the past are condemned to repeat it."
George Santayana

- Two faults in Oregon (500 kV & 230 kV) led to …
  - Tripping of generators at McNary dam
  - 500 MW oscillations
  - Separation of the Pacific Intertie at the California-Oregon border
  - Blackouts in 13 states/provinces
- Some studies show with proper "intelligent controls," all would have been prevented by shedding 0.4% of load for 30 minutes!


Sunday, August 11, 1996

Millions lose power

Half of PG&E's customers in Northern California affected; blackouts in 9 states

U.S. says power will be bolstered

Outage raises serious worries

Firms wonder: Is this the future?

More Outages Expected for Power Network

Investigations planned after power grid falters

ELECTRICITY USERS FEELING POWERLESS

August 10, 1996

Everyone wants to operate the power system closer to the edge. A good idea! But, ***where is the edge and how close are we to it?***

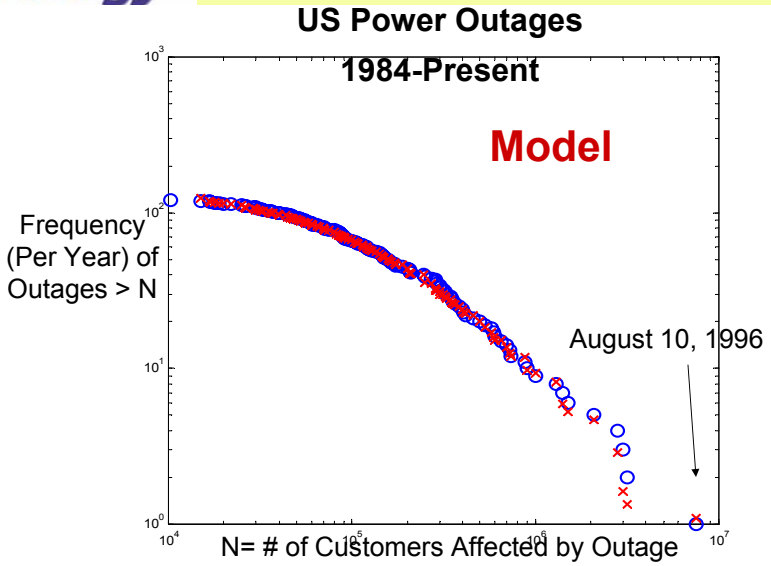
CIN/SI Funded Consortia

107 professors in 28 U.S. universities are funded: Over 360 publications, and 19 technologies extracted, in the 3-year initiative

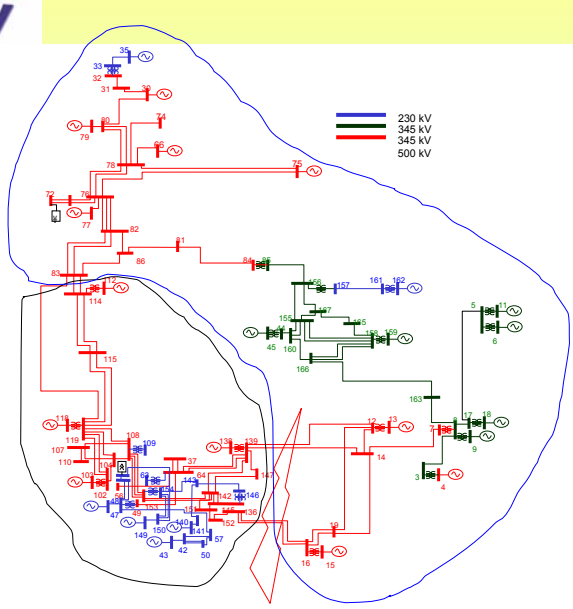
- U Washington, Arizona St., Iowa St., VPI
- Purdue, U Tennessee, Fisk U, TVA, ComEd
- Harvard, UMass, Boston, MIT, Washington U.
- Cornell, UC-Berkeley, GWU, Illinois, Washington St., Wisconsin
- CMU, RPI, UTAM, Minnesota, Illinois
- Cal Tech, MIT, Illinois, UC-SB, UCLA, Stanford

- Defense Against Catastrophic Failures, Vulnerability Assessment
- Intelligent Management of the Power Grid
- Modeling and Diagnosis Methods
- Minimizing Failures While Maintaining Efficiency / Stochastic Analysis of Network Performance
- Context Dependent Network Agents
- Mathematical Foundations: Efficiency & Robustness of Distributed Systems

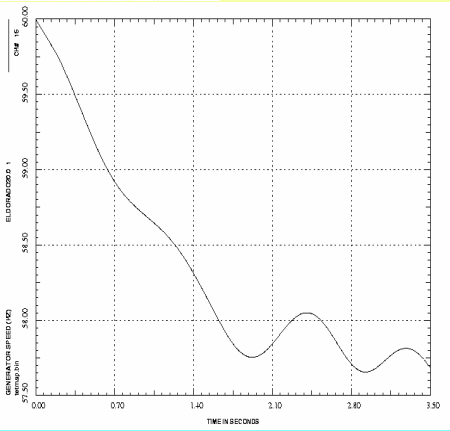
Complex Interactive Networks Initiative: Power Laws

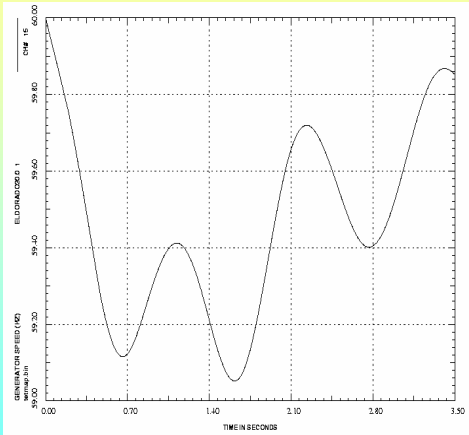


Adaptive Islanding



Simulation Result

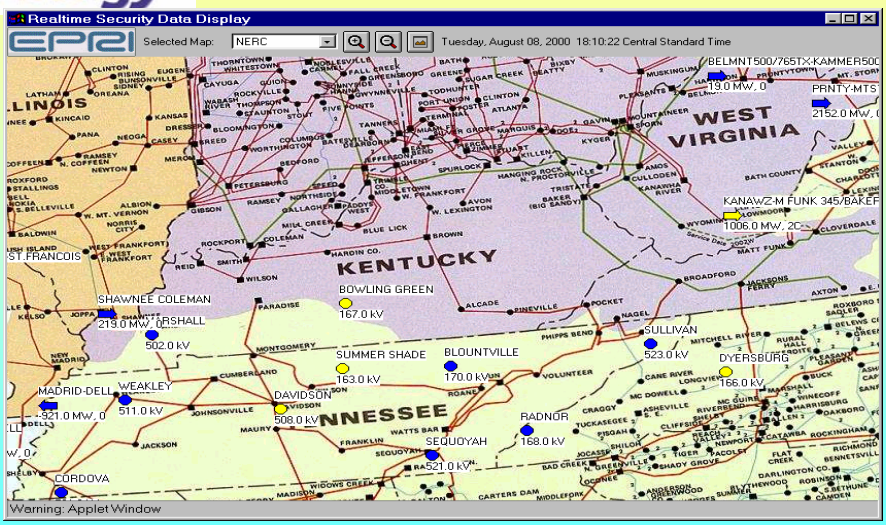




No Load Shedding Scheme

New Scheme

Reliability Initiative-- Sample Screen of Real-time Security Data Display (RSDD)



The Threat:
Aftermath of the 9/11 Tragedies

- **Electric power systems constitute *the* fundamental infrastructure of modern society and therefore an inviting target for three kinds of terrorist attacks:**
- **Attacks upon the system**
  - **Power system itself is primary target with ripple effect throughout society**
- **Attacks by the system**
  - **Population is the actual target, using parts of the power system as a weapon**
- **Attack through the system**
  - **Utility networks provide the conduit for attacks on broad range of targets**

Steps Toward Ensuring Security

- **EPRI's *Electricity Infrastructure Security Assessment* considers six broad areas:**
  - **System-Wide Vulnerability Assessment**
  - **Grid Security**
  - **Cyber and Communications Threats**
  - **Distribution System, Disaster Mitigation & Recovery**
  - **Generation/Environment**
  - **Power Markets**

ISI Areas: Determining System Vulnerability to Various Attack Modes, Reducing Their Impact, and Rapid Recovery

- Strategic Spare Parts Inventory: Reducing recovery time from terrorist attack or natural disaster by providing spare parts of existing equipment and by developing standardized "recovery transformers" with multiple voltage taps
- Vulnerability Assessment (VA): Determining the impact of potential terrorist attacks on power system components throughout the end-to-end electricity supply chain
- "Red Team" Attacks: Launch mock assaults on the computer and information networks of selected utility systems, probing for weaknesses in a manner similar to the FAA's Red Team efforts
- Secure Communications: Scoping study to determine how to develop a secure, private communications network for the electric power industry, as an alternative to Internet-based systems

Coordination with Ongoing Programs

- Presidential Directive #63, issued in May 1998: NERC designated as the ISAC (Information Sharing and Analysis Center) for the electricity sector.
- Increased coordination with NERC and the Electric power industry trade associations – including EEI, NRECA, APPA, NEMA, NECA, …
- White House Office of Homeland Security (OHS) and Office of Science and Technology Policy (OSTP), and DHS
- DOE, Office of Critical Infrastructure Protection (DOE-CIP), and National Laboratories
- Department of Defense (DDR&E); Institute for Defense Analyses (IDA)
- National Science Foundation (NSF)
- U.S. National Academy of Engineering (NAE)
- Department of Commerce, Critical Infrastructure Assurance Office (CIAO) and National Infrastructure Protection Center (NIPC)
- Department of State

Observations

- Tactical response is adequate, but strategic response is lacking
- There is no centralized industry security coordination and assurance capability
- A supportive public policy umbrella is needed
- The public doesn't appreciate the latent threat to the power system

Discussion Questions

- What level of threat is the industry responsible for, and what does government need to address?
- Will market-based priorities support a strategically secure power system?
- What system architecture is most conducive to maintaining security?

Conclusions

- Utility Systems are tempting targets
- Cyber attacks are very probable
- We know what we need to do to prevent & mitigate attacks
- The industry and government are working on solutions with a sense of urgency, and a lot remains to be done.
- We will be successful!